UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

I.C., ET AL.,

Plaintiffs,

vs.

ZYNGA, INC.,

Defendant.

CASE NO. 20-cv-01539-YGR

ORDER GRANTING MOTION TO DISMISS

Re: Dkt. No. 96

Plaintiffs bring this consolidated putative class action against social gaming company Zynga Inc. in connection with a large-scale data breach of players' account information. The Court previously granted Zynga's motion to dismiss the first consolidated class action complaint for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure ("Rule") 12(b)(1), permitting plaintiffs to amend their pleadings. Currently pending is Zynga's motion to dismiss the second consolidated class action complaint ("SAC") on the same basis. (Dkt. No. 96.) Having carefully reviewed the pleadings and the briefing on the motion, and for the reasons stated below, the Court hereby **GRANTS** the motion **WITHOUT LEAVE TO AMEND**.[1]

I. BACKGROUND

The SAC (Dkt. No. 95) alleges as follows:

Zynga develops, markets, and operates live social games including the popular *Words With Friends* and *Farmville* franchises. (SAC ¶ 42.) These games are played on the Internet, social networking sites, and mobile platforms "by millions of people around the world each day." (*Id.*) Plaintiffs were among such players. (*Id.* ¶¶ 8–37.) Zynga offers a mix of paid and free games to players while also providing advertising services to advertising agencies and brokers. (*Id.* ¶¶ 42, 44.) The free games are supported by in-game advertisements, in-game purchases, and Zynga's collection and sale of users' personal identifying information ("PII"). (*Id.* ¶ 44.)

One must create an account with Zynga to play its games. (*Id.* ¶ 47.) "In connection with

[1] Pursuant to Federal Rule of Civil Procedure 78(b) and Civil Rule 7-1(b), the Court finds this motion appropriate for decision without oral argument.

the account creation process, Zynga collects certain PII from users, including their first name, last name, email address, gender, and a password for the account, if one was created." (*Id.* ¶ 48.) Users "have the option to link their Zynga account to their Facebook account instead of providing an email address. If a prospective user chooses to log in with Facebook, the prospective user must provide their Facebook username and/or phone number and password through a separate authentication screen." (*Id.* ¶ 49.) The SAC further alleges, "[u]pon information and belief, before it began using a third-party payment processor, Zynga collected financial information, such as credit card details, for game purchases or in-app purchases." (*Id.* ¶ 50.)

On September 12, 2019, Zynga posted on its website the following statement, titled "Player Security Announcement," which stated in relevant part:

> We recently discovered that certain player account information may have been illegally accessed by outside hackers. An investigation was immediately commenced, leading third-party forensics firms were retained to assist, and we have contacted law enforcement.
>
> While the investigation is ongoing, we do not believe any financial information was accessed. However, we have identified account login information for certain players of *Draw Something* and *Words With Friends* that may have been accessed. As a precaution, we have taken steps to protect these users' accounts from invalid logins. We plan to further notify players as the investigation proceeds.

(*Id.* ¶ 84.) Zynga "never notified those customers by email, or even by a pop-up notification" regarding the data breach or "offer[ed] any assistance with mitigating the risks associated with same." (*Id.* ¶¶ 12, 86.)

On September 29, 2019, The Hacker News reported that a serial hacker breached Zynga's customer database and acquired the information of more than 218 million users. (*Id.* ¶ 67.) The hacker reported that the breach affected all Android and iOS game players who had installed and signed up for the *Words With Friends* game on or before September 2, 2019. (*Id.*) The SAC alleges that the affected users' PII have been sold or otherwise published on the dark web. (*Id.* ¶ 114.)

According to the SAC, identity theft can occur by using the PII stolen from Zynga. (*Id.* ¶

95.) For example, a cyber attacker can take "a massive trove of usernames and passwords from a data breach and tr[y] to 'stuff' those credentials into the login page of other digital services." (*Id.* ¶ 97.) "The vast majority of email and password comb[inations] [will not] work, but a few will. That[is] because many people reuse the same credentials on multiple websites." (*Id.* ¶ 103 (internal quotation marks and citation omitted).) In addition to these so-called credential stuffing attacks, the breached data includes "enough information for hackers to potentially create targeted phishing attacks made up to look as if they are an official communication from Zynga." (*Id.* ¶ 101 (internal quotation marks and citation omitted).) "The communications can also look like they are from other trusted companies, such as banks, and claim that there is suspicious activity on the account to tempt a person to click on a link and provide additional valuable PII." (*Id.* (citation omitted).) The information stolen from Zynga is "highly valued amongst cyber thieves and criminals," creating a "well-established market" on the dark web. (*Id.* ¶ 96.) The SAC cites a number of reports describing the financial, emotional, and physical injuries that victims of identity theft can suffer, particularly for minors, who comprise "a substantial portion of [Zynga's] user base." (*Id.* ¶¶ 59–64, 131–38.)

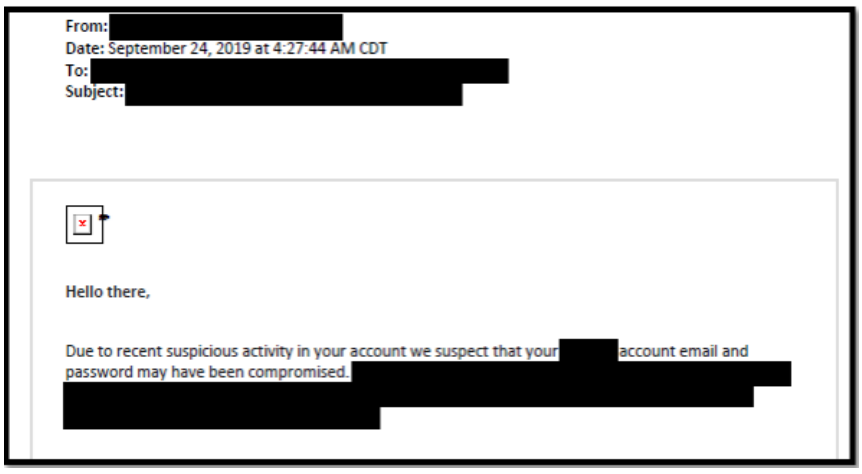
The SAC is not entirely consistent regarding the information stolen in the breach. At minimum, the information allegedly stolen included names, email addresses, phone numbers, Zynga usernames, Zynga passwords (some hashed and some in plain text), Zynga password reset tokens, and Facebook usernames. (*Id.* ¶ 67.) The SAC includes gender, home address, and credit card information in the definition of "PII" but does not specifically allege that this data was taken in the breach. (*Compare id.* ¶ 2 n.1 *with id.* ¶ 67.) The SAC also alleges that the stolen information included "dates/times when the account was created, last accessed, and the IP address of the last login," but did not include such information in the PII definition. (*Compare id.* ¶ 67 *with id.* ¶ 2 n.1.) In addition, the SAC alleges both that users' dates of birth were stolen but also that Zynga did not collect information regarding a user's age or date of birth. (*Compare id.* ¶ 2 n.1 *with id.* ¶ 48.) Further, while alleging that Facebook passwords were stolen, the SAC also alleges that Zynga reportedly does not collect Facebook passwords and that the hacker only claimed to have accessed "the 'Facebook IDs' of Zynga users." (*Compare id.* ¶ 2 n.1 *with id.* ¶ 68.)

Named plaintiffs are Zynga players whose information was allegedly hacked during the breach: I.C., Amy Gitre, Carol Johnson, Lisa Thomas, Joseph Martinez IV, Daniel Petro, and Christopher Rosiak. (*Id.* ¶¶ 8, 14, 16, 23, 25, 27, 31.) The Court previously granted Zynga's motion to compel arbitration of the claims of Gitre, Thomas, and Martinez. (Dkt. No. 93.) With respect to the remaining plaintiffs, the following information was allegedly stolen:

- Petro: email address and Zynga username
- I.C.: email address, Zynga username, and Zynga password
- Johnson: email address, Zynga username, *Games with Friends* hashed password, *Draw Something* plain text password, date of birth, phone number, and Zynga password reset tokens
- Rosiak: email address, Zynga username, Zynga password, phone number, Facebook name, and Facebook username

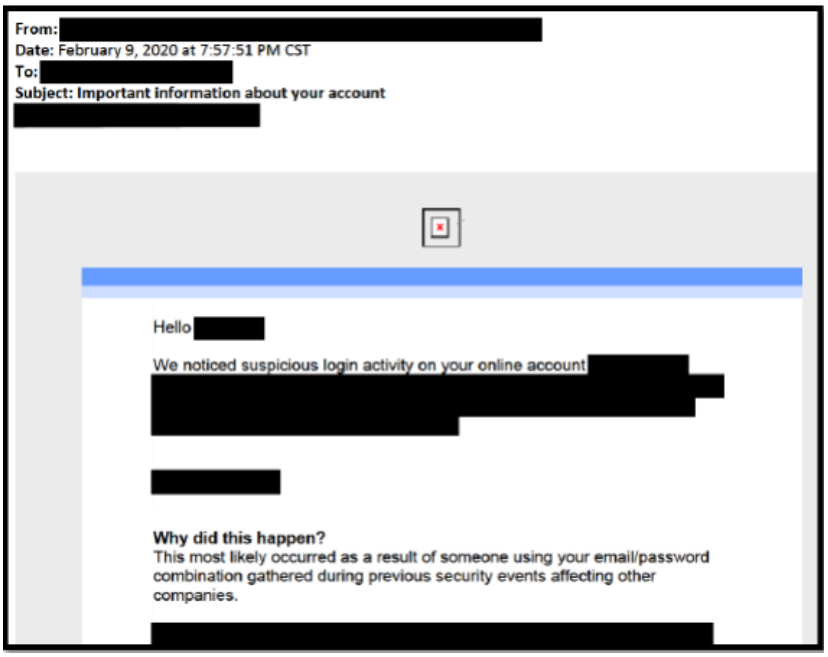
(*Id.* ¶¶ 10, 19, 30, 31.) The only plaintiff that allegedly had their Zynga password stolen in plain text form is Johnson. (*Id.* ¶¶ 19, 74.) Zynga did not directly notify these plaintiffs that their information had been compromised by the breach. (*Id.* ¶¶ 8, 17, 29, 34.) I.C., Johnson, and Petro confirmed through the website haveibeenpwned.com, and Rosiak received notices from an identity theft monitoring service, about the same. (*Id.* ¶¶ 8, 17, 29, 34–35, 120–121.)

In the aftermath of the data breach, each of the named plaintiffs allege they were affected by the breach in a number of ways. I.C., who is a minor, received at least three notices regarding non-Zynga accounts indicating that I.C.'s login information may be compromised, reproduced below.


From: [redacted]
Date: September 24, 2019 at 4:27:44 AM CDT
To: [redacted]
Subject: [redacted]

Hello there,

Due to recent suspicious activity in your account we suspect that your [redacted] account email and password may have been compromised. [redacted]



(*Id.* ¶¶ 106, 109, 112.) Two of those notices concerned other gaming accounts.

I.C. also received at least two suspicious emails, including one from Personal Capital, reproduced below.

From: Mary <[redacted]>
Date: November 16, 2019 at 4:31:02 PM CST
To: "[redacted]" <[redacted]>
Subject: Re: [redacted]

Evening
is it [redacted]?

From: Personal Capital <service@personalcapital.com>
Date: October 29, 2019 at 8:35:47 PM CDT
To: [redacted]
Subject: A Message From Our CMO
Reply-To: Personal Capital <service@personalcapital.com>

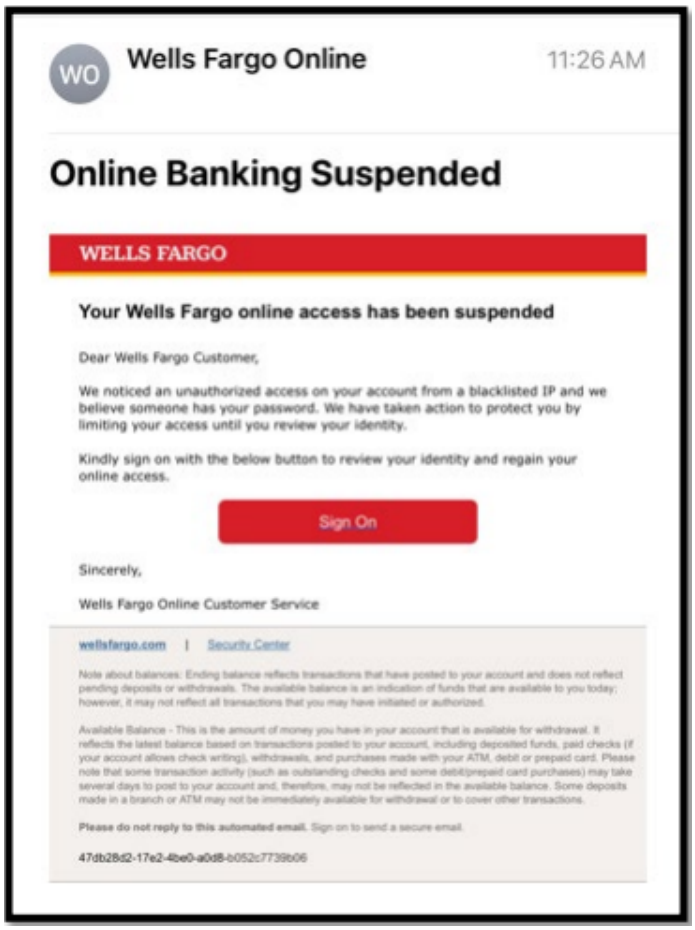
Hi,

We are endlessly thankful to you for trusting us and for using Personal Capital's financial tools. Today marks our ten-year anniversary and we wouldn't be here without you. To celebrate our birthday we are introducing an updated look that more closely represents who we are as a company and what we believe in.

(*Id.* ¶¶ 107, 111.) I.C. has no knowledge or experience with Personal Capital, which markets itself as an online financial advisor and personal wealth management company. (*Id.* ¶ 111.) I.C. "used his Zynga password for approximately 90% of his online accounts, including email, entertainment, gaming, social media popular with youth, and others." (*Id.* ¶ 105.) After learning of the data breach in January 2020, I.C. "spent hours attempting to update his account passwords"

and "install[ing] a two-factor authentication application" but could not be certain that he did so for all of his accounts. (*Id.* ¶¶ 116–18.)

Rosiak was "inundated" with suspicious email, calls and texts. (*Id.* ¶¶ 125, 129.) One such text was addressed to "Henry," which is the first name of his fake Facebook account. (*Id.* ¶ 129.) He also received an email purportedly from Wells Fargo, reproduced below, that was "likely a phishing email."



(*Id.* ¶ 128.) Rosiak never had a Wells Fargo banking account. (*Id.*) In addition, he received Facebook "friend suggestions" and "people you may know" from individuals, none of whom he knew or had any connection. (*Id.* ¶ 126.)[2] Rosiak "spent considerable time changing all of his

[2] The SAC includes the screenshots of these individuals as well as their names (Mirazad Mirazad, UMii Aiman, Ubb Ibaid, Riya Mandal, Awara Ladka, B Hat Zurjn, MaHi INhu, and Eshutosh Paikra) and notes that the hacker is from Pakistan. (Compl. ¶ 126.) The Court declines to speculate as to what inference plaintiffs are attempting to draw.

passwords," deleted his Facebook account, changed his voice mail message to a generic message that did not reveal his first name, and experienced "considerable alarm, stress and concern." (*Id.* ¶¶ 125, 127, 129, 130.)

Johnson, who is a septuagenarian and "not particularly computer-savvy," experienced an increase in phishing emails. (*Id.* ¶¶ 20, 21.) She also "used the same password she provided to Zynga for many other online accounts, including her email account which she uses to send confidential information such as financial information and communications with her doctor's office." (*Id.* ¶ 20.) Johnson "spent at least three to four hours in an attempt to mitigate . . . against the risk of identity theft and fraud upon learning the Zynga data breach." (*Id.*) She and her sister "went through every online account she could think of that had the same password as her Zynga account in an attempt to change the passwords." (*Id.*) The foregoing has caused her "considerable alarm, stress, and concern." (*Id.* ¶ 22.)

Petro received Facebook friend requests from individuals with whom he had no connection. (*Id.* ¶ 30.) He also received multiple spam and robo calls on the phone he uses to access his Zynga account. (*Id.*)

Beginning in March 2020, plaintiffs individually filed putative class actions against Zynga in connection with the September 2019 data breach. Zynga filed motions to compel arbitration in three of the four actions based on the mandatory arbitration provision in the applicable terms of service. Because it was unclear which terms plaintiffs accepted, the Court denied the motions but directed plaintiffs to provide their contact information to enable Zynga to review plaintiffs' Zynga accounts. (Dkt. No. 60.) After consolidation of the actions, plaintiffs filed a consolidated class action complaint. (Dkt. No. 67.) Thereafter, Zynga filed a renewed motion to compel arbitration as well as a motion to dismiss the FAC for lack of subject matter jurisdiction under Rule 12(b)(1) and for failure to state a claim under Rule 12(b)(6). (Dkt. Nos. 71, 72.) Upon hearing arguments, the Court granted the motion to compel as to Gitre, Thomas, and Martinez, as well as the motion to dismiss. (Dkt. No. 93.) The Court permitted plaintiffs to file an amended complaint and permitted defendants, should they again move to dismiss under Rule 12(b)(1), to defer any Rule 12(b)(6) challenges.

The SAC alleges 29 causes of action under state common and statutory law, some of which are asserted in pairs (respectively brought by the minor plaintiff and the other plaintiffs): negligence (counts I and II); negligence per se (counts III and IV); negligent misrepresentation (counts V and VI); breach of contract (counts VII and counts VIII); unjust enrichment (counts IX and X); breach of confidence (count XI); violation of state data breach statutes (counts XII and XIII); intrusion upon seclusion (counts XIV and XV); declaratory judgment (counts XVI and XVII); violations of California Unfair Competition La (count XVIII), California False Advertising Law (count XIX), California Consumers Legal Remedies Act (count XX), Missouri Merchandising Practices Act (count XXI), Wisconsin Deceptive Trade Practices Act (count XXII), Colorado Consumer Protection Act (count XXIII), Iowa Consumer Fraud Act (count XXIV), Indiana Deceptive Consumer Sales Act (count XXV), Kansas Consumer Protection Act (count XXVI), and Michigan Consumer Protection Act (XXVII); and publicity given to private life (counts XXVIII and XXIX). The SAC alleges that Zynga failed to protect its customers' PII by, among other things, using outdated password encryption methods that were banned for use by federal government agencies as early as 2010. (SAC ¶ 3.)

Zynga now moves to dismiss the SAC for lack of subject matter jurisdiction under Rule 12(b)(1). Specifically, Zynga contends that plaintiffs fail to allege a concrete injury in fact such that they cannot establish Article III standing to pursue this action in federal court.

II. LEGAL STANDARD

Federal courts are courts of limited jurisdiction. Article III of the Constitution "confines the federal judicial power to the resolution of 'Cases' and 'Controversies.'" *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). "For there to be a case or controversy under Article III, the plaintiff must have a 'personal stake' in the case – in order words, standing." *Id.* (citation and quotation marks omitted). To establish standing, a "[p]laintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo v. Robins*, 578 U.S. 330, 338 (2016). Here, traceability and redressability are not at issue.

"To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a

legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* at 339 (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992)). The critical inquiry raised by Zynga is whether the injuries alleged are concrete. A "concrete" injury may include tangible or intangible harms, so long as they "actually exist" and are "'real,' and not 'abstract.'" *TransUnion*, 141 S. Ct. at 2204 (quoting *Spokeo*, 578 U.S. at 340). A real, existing injury is a prerequisite to federal jurisdiction because "federal courts do not adjudicate hypothetical or abstract disputes," nor do they "exercise general legal oversight . . . of private entities." *Id.* at 2190.

The Court evaluates challenges to Article III standing under Rule 12(b)(1), which governs motions to dismiss for lack of subject matter jurisdiction. *See Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011) (motion to dismiss for lack of standing governed by Rule 12(b)(1)). Rule 12(b)(1) motions may be either facial, where the inquiry is confined to the allegations in the complaint, or factual, where the court is permitted to look beyond the complaint to extrinsic evidence. *See Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014); *Safe Air For Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). When a defendant challenges jurisdiction "facially," all material allegations in the complaint are assumed true, and the court determines whether the factual allegations are sufficient to invoke the court's subject matter jurisdiction. *See Leite*, 749 F.3d at 1121; *Meyer*, 373 F.3d at 1039. When a defendant makes a factual challenge "by presenting affidavits or other evidence properly brought before the court, the party opposing the motion must furnish affidavits or other evidence necessary to satisfy its burden of establishing subject matter jurisdiction." *Meyer*, 373 F.3d at 1039; *see also Leite*, 749 F.3d at 1121. The court need not presume the truthfulness of the plaintiff's allegations under a factual attack. *Wood v. City of San Diego*, 678 F.3d 1075, 1083 n.2 (9th Cir. 2011). The plaintiff must show by a preponderance of the evidence each requirement for subject-matter jurisdiction, and as long as the dispute is not intertwined an element of the plaintiff's cause of action, the court may resolve any factual disputes itself. *Leite*, 749 F.3d at 1121.

Zynga purports to mount a factual attack by relying on the declaration of Zynga's technical director filed in support of its first motion to dismiss. (Motion to Dismiss the SAC ("Mtn."), Dkt.

No. 96, at 1 (citing Declaration of Jessup Ferris in Support of Motion to Dismiss, Dkt. No. 72-12.).) Although the instant motion cites to the Ferris declaration, the jurisdictional inquiry below does not turn on any factual dispute. Accordingly, the Court construes the 12(b)(1) motion as a facial attack.

In a class action, at least one named plaintiff must have standing. *See Frank v. Gaos*, 139 S. Ct. 1041, 1046 (2019); *Ollier v. Sweeetwater Union High Dist.*, 768 F.3d 843, 865 (9th Cir. 2014). Thus, "if none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendant[ ], none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974). Moreover, standing must be established "for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)." *TransUnion*, 141 S. Ct. at 2208. Because plaintiffs are the parties invoking federal jurisdiction, they "bear[ ] the burden of establishing these elements." *Spokeo*, 578 U.S. at 338 (citing *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231 (1990)). In the absence of standing, there is no subject matter jurisdiction. *See Bender v. Williamsport Area Sch. Dist.*, 475 U.S. 534, 546–47 (1986) (citing *Mansfield C. & L.M.R. Co. v. Swan*, 111 U.S. 379, 382 (1884)).

III. ANALYSIS

As noted above, plaintiffs seek both damages and injunctive relief for 29 causes of action under state statutory and common law. According to plaintiffs, they allege the following forms of harm: (i) a "present, increased risk" of identity theft; (ii) time spent mitigating said risk; (iii) emotional distress; (iv) diminution in value of their PII; and (v) loss of privacy. (Opposition to Motion to Dismiss ("Opp."), Dkt. No. 98, at 9–24.)[3] Plaintiffs argue that each of these alleged injuries confers Article III standing.

Zynga contends that because plaintiffs have not demonstrated that the alleged harms are

[3] The harms described in plaintiffs' opposition brief do not track the laundry list of injuries alleged in the SAC; nor do plaintiffs associate each of the alleged injuries with each of the claims. (*See* Compl. ¶¶ 139, 141–42, 183.) The Court declines to scour the 101-page pleading to do the same. Instead, the Court considers the alleged harms as described in plaintiffs' opposition brief and assumes, for plaintiffs' benefit, that all of the counts are premised on each of the alleged injuries.

concrete, they fail to establish an injury in fact and therefore lack Article III standing. Specifically, Zynga argues that plaintiffs cannot demonstrate standing: (1) based on the alleged risk of identity theft; (2) based on the alleged loss of privacy; and (3) for injunctive relief. As explained below, the other injuries alleged (mitigation costs, emotional distress, and diminution in value) rise and fall with the alleged risk of identity theft. Before evaluating these alleged injuries, the Court begins its analysis by observing recent guidance from the Supreme Court about whether an alleged harm is adequately concrete so as to confer Article III standing.

A. *TRANSUNION LLC V. RAMIREZ*

In *TransUnion LLC v. Ramirez*, a class of plaintiffs sued the credit reporting company under the Fair Credit Reporting Act because their credit reports misleadingly labeled them as potential terrorists. *TransUnion*, 141 S. Ct. at 2200–02. TransUnion, however, provided the inaccurate reports to third parties for only a subset of plaintiffs. *Id.* The Supreme Court held that these plaintiffs suffered harm akin to defamation, enabling them to maintain their claims. *Id.* at 2209; *see id.* at 2204 ("courts should assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts") (quoting *Spokeo*, 578 U.S. at 341).

However, the same could not be said about the remaining plaintiffs whose credit reports TransUnion had never published to others. According to the Court, because defamation requires evidence of publication, which is traditionally "presumed to cause a harm, albeit not a readily quantifiable harm," those plaintiffs' failure to allege dissemination was fatal to their traditional-harm theory. *Id.* at 2211. In other words, "the mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party," does not closely resemble the harm associated with common law defamation and therefore "causes no concrete harm." *Id.* at 2210.

Nor could that group of plaintiffs suffer a concrete injury based on the risk of harm where such risk of harm did not materialize (that is, dissemination of the inaccurate credit reports to third parties) or cause some other injury. *Id.* at 2211. The Supreme Court explained that "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *Id.* at

2210 at (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5). However, where a plaintiff brings "a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm." *Id.* at 2210–11.

B. ALLEGED INJURIES IN FACT

Plaintiffs assert both theories of injury-in-fact discussed in *TransUnion*: a harm traditionally recognized at common law as well as a risk of harm (or in plaintiffs' words, a "present, increased risk of harm"). The Court considers each in turn, beginning with the former.

1. TRADITIONAL HARM: INVASION OF PRIVACY

In *TransUnion*, the Supreme Court instructed that "courts should assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts," such as physical harm, monetary harm, or various intangible harms. *Id.* at 2204. Concrete intangible harms "include, for example, reputation harms, disclosure of private information, and intrusion upon seclusion." *Id.* (citations omitted). This inquiry focuses on "whether plaintiffs have identified a close historical or common-law analogue for their asserted injury . . . but does not require an exact duplicate in American history or tradition." *Id.* In addition to history, "Congress's views may be 'instructive.'" *Id.* (quoting *Spokeo*, 578 U.S. at 341).

Plaintiffs submit that they allege invasions of privacy bearing a close relationship to harms caused by the common law private torts of disclosure of private facts and intrusion upon seclusion. As to the public disclosure of private facts, "[o]ne who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not a legitimate concern to the public." Restatement (Second) of Torts § 652D. A plaintiff whose private life is given publicity "may recover for the harm resulting to his reputation from the publicity." *Id.* § 652H. As to intrusion upon seclusion, "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly

offensive to a reasonable person." *Id.* § 652B. A plaintiff who suffers an intrusion upon seclusion "may recover damages for the deprivation of his seclusion." *Id.* § 652H.

Zynga challenges plaintiffs' reliance on these traditional harms, arguing that plaintiffs fail to adequately allege (1) the disclosure of private facts and (2) publicity. The Court notes that for both torts, the harm is caused by the disclosure of or intrusion upon matters of a kind that would be "highly offensive to a reasonable person." Even viewing the allegations in the light most favorable to plaintiffs, the Court finds that the type of harm they suffered as a result of the data breach is not analogous to the type of harm suffered as a result of private information. Plaintiffs have not demonstrated that the information stolen was of a nature that disclosure or intrusion thereupon would be highly offensive to the reasonable person. *Cf. TransUnion*, 141 S. Ct. at 2209 ("The harm from being labeled a 'potential terrorist' bears a close relationship to the harm from being labeled a 'terrorist.'"). The Court reasons:

First, the Court is hard pressed to conclude that basic contact information, including one's email address, phone number, or Facebook or Zynga username, is private information. All of this information is designed to be exchanged to facilitate communication and is thus available through ordinary inquiry and observation. Next, "there is no liability for giving publicity to facts about the plaintiff's life that are matters of public record, such as the date of his birth[.]" Restatement (Second) of Torts § 652D, Comment b. Finally, assuming it is not encrypted, the Zynga password presents a closer question as passwords generally are confidential. However, under the circumstances of this case, it is not clear to the Court, nor do plaintiffs explain, how the discovery of a password to a gaming account would be "highly offensive to a reasonable person,"[4] particularly where there is no allegation that the gaming accounts for which plain text passwords were taken contain confidential information.[5] It is also worth noting that plaintiffs do not allege that any of their actual first or last names were exposed in the data breach, suggesting that their

[4] For example, will a player be offended if others learned their *Words With Friends* statistics?

[5] Whether the password can be used to commit identity theft is a different matter discussed in the next section.

anonymity is preserved.[6] Moreover, with the exception of a date of birth, which is immutable, all of this information can be changed. Even when these pieces of information are considered holistically, the Court does not view the collection of email addresses, phone numbers, Zynga usernames, Zynga passwords, and Facebook usernames so private that their revelation would be highly offensive to a reasonable person.[7]

In sum, while plaintiffs are not required to prove the elements for a common-law analogue in order to secure standing,[8] they must demonstrate that the harm posed by the theft of their information bears a "close relationship" to these traditionally recognized harms. *Cf TransUnion*, 141 S. Ct. at 2209 ("[T]he harm from a misleading statement of this kind bears a sufficiently close relationship to the harm from a false and defamatory statement."). Here, plaintiffs broadly assert that "a combination of multiple categories information can convey a wealth of information and seriously implicate privacy rights." (Opp. at 22.)[9] However, in data breach cases, courts must examine the nature of the specific information at issue to determine whether privacy interests were implicated at all. Otherwise, every data breach (or any situation in which one loses control of information) would confer standing, regardless of whether private information is exposed.

For the reasons stated above, the Court finds an insufficient fit between the loss of information alleged here and the common law privacy torts of private disclosure of private facts

---

[6] Rosiak's Facebook name was also allegedly taken, but he even concedes that he used a fake first name on his Facebook profile. (SAC ¶ 121.)

[7] In their brief, plaintiffs make no mention of any privacy interests in the password reset tokens, dates and times when the account was created and last accessed, or the IP address of the last login. The Court will not address an issue not briefed by the parties.

[8] Nor are they required to demonstrate additional consequences from the invasion of privacy, once shown, because the invasion itself constitutes the alleged injury in fact.

[9] The Court is not persuaded by plaintiffs' reliance on cases involving the disclosure of a plaintiff's name and alleged debt to a third party. (Opp. at 20 (citing *Hunstein v. Preferred Collection & Mgmt. Servs.*, 994 F.3d 1341, 1347 (11th Cir. 2021), *Thomas v. Unifin, Inc.*, No. 21-cv-3037 (SJC), 2021 WL 3709184 (N.D. Ill. Aug. 20, 2021), and *Keller v. Northstar Location Servs.*, No. 21-cv-3389 (SJC), 2021 WL 3709183 (N.D. Ill. August 20, 2021).) All are factually distinguishable. Plaintiffs' names were not alleged to be stolen, and their contact information, date of birth, and password for a gaming account are distinguishable from the fact and amount of one's debt.

and intrusion upon seclusion. Therefore, the Court agrees with Zynga that the privacy injuries alleged here are not sufficiently concrete to provide the basis for Article III standing.[10]

2. RISK OF HARM

a. STANDING TO SUE FOR DAMAGES

Zynga also argues that, in light of *TransUnion*, plaintiffs cannot rely on a "mere risk of future harm" as a basis for standing. Plaintiffs contend that they allege more than a mere risk of future harm but rather they allege a "present, increased risk" of harm. In the Court's view, plaintiffs are drawing a distinction without a difference. Nowhere in *TransUnion* does the Supreme Court use this language or otherwise distinguish between a present risk of harm and a future risk of harm.[11] The point made by the Supreme Court is that a "pre-existing" risk of harm cannot confer Article III standing in a suit for damages. *See TransUnion*, 141 S. Ct. at 2211 (risk of harm, by itself, is not a sufficiently concrete injury). Thus, to the extent that plaintiffs base standing on a (present) risk of identity theft, they cannot pursue their claims for damages.

The Supreme Court explained that a risk of harm must either *materialize* or *cause some other injury* in order to confer standing in a suit for damages. *See id.* The Court therefore considers whether plaintiffs do, in fact, "allege more than" a risk of harm. Specifically, the Court evaluates whether the asserted risk of harm, here, identity theft, materialized or caused some other injury.

i. MATERIALIZATION OF RISK: ACTUAL IDENTITY THEFT

Plaintiffs argue that "the alleged risk of harm has actually materialized for" them. (Opp. at

---

[10] Because the Court concludes that the disclosure and intrusion here are not highly offensive to a reasonable person, it necessarily finds that private facts are not at issue and therefore need not address Zynga's challenge regarding plaintiffs' purported failure to allege publicity. Nevertheless, even if the highly-offensive component were not met, the Court questions whether plaintiffs could establish that their alleged harm bears a "close relationship" with the harm resulting from a public disclosure of private facts without any showing of "harm to their reputation from the publicity," assuming publicity occurred here. Moreover, plaintiffs allege that a third-party hacker, not Zynga, stole their information and therefore it is doubtful whether they can show that Zynga (whom plaintiffs sue for negligence) directly harmed them in a way that is analogous to the harm from *intentional* intrusion upon seclusion.

[11] If there is a risk of some event, then there is a currently existing possibility that that event will occur in the future.

6.) The Court disagrees. The harm to which plaintiffs refer is identity theft (or fraud). Thus, the materialization of the risk of identity theft is *actual* identity theft, not *attempted* identity theft. *See id.* ("[T]he 6,332 plaintiffs did not demonstrate that the risk of future harm materialized—that is, that the inaccurate OFAC alerts in their internal TransUnion credit files were ever provided to third parties or caused a denial of credit.").[12]

Here, the SAC does not allege that any of the plaintiffs actually experienced any type of fraud or identity theft as a result of the data breach, such as the unauthorized access of an account or the unauthorized transaction made in their name. Notwithstanding, plaintiffs argue that their information "has been used to compromise their other accounts with credential stuffing, to establish new accounts in their names, to entice them with phishing emails from purported banks and brokerage companies, to lure them with personal emails meant to look like a personal conversation, and to bombard them with spam calls and texts." (Opp. at 1.) As an initial matter, in light of *TransUnion*, the Court concludes that mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft. Moreover, the Court finds that being "entice[d]" or "lure[d]" into giving information that can be used to commit fraud is not the same thing as actually being defrauded. Further, the Court agrees with other courts that "receiving spam or mass mail does not constitute an injury in fact." *See*, *e.g.* *Jackson v. Loews Hotels, Inc.*, No. 18-cv-827 (DMG), 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) (citing cases including *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) ("The receipt of spam by itself . . . does not constitute a sufficient injury entitling [the plaintiff] to compensable relief.")).

Finally, the SAC does not plausibly allege that unauthorized accounts were established in any of the plaintiffs' names. Plaintiffs argue that "I.C.'s identity has already been stolen to set up fraudulent accounts with financial information." (Opp. at 12 (citing SAC ¶ 11 and related

[12] The Court is not persuaded by plaintiffs' characterization of attempted identity theft as actual misuse of their stolen information. (Opp. at 8 ("Plaintiffs assert damages based on ***actual misuse*** of their PII by cybercriminals attempting to commit identity theft and fraud—a ***present*** risk of harm."), 12 ("Plaintiffs' PII *has already been misused*—specifically, to target Plaintiffs in an attempt to commit identity theft and fraud.").)

screenshot).) Putting aside the fact that the SAC does not plausibly allege that any of I.C.'s information stolen in the data breach could be used to set up an account with a financial institution, such as a social security number, nothing in the non-personalized message, reproduced above, plausibly suggests that I.C.'s identity was actually stolen to create a fraudulent account. The Court also notes that the SAC contains vague allegations regarding "unauthorized access to and misuse of their accounts, "lowered credit scores resulting from credit inquiries and caused by fraudulent activities," and "unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit." (SAC ¶¶ 142 (d), (e), 183(d).) However, the SAC does not allege that any of the plaintiffs actually experienced any of these adverse consequences, information that they would presumably know especially given that the breach occurred at the end of 2019 and the most recent version of the complaint was filed at the end of August 2021.

Therefore, because plaintiffs do not allege any actual identity theft or fraud, they cannot claim an injury in fact based on a materialization of the risk of harm. *See TransUnion*, 141 S. Ct. at 2211.

ii. OTHER INDEPENDENT INJURIES CAUSED BY RISK OF HARM

Plaintiffs also do not plausibly allege other independent injuries caused by the risk of identity theft. Plaintiffs cite the following as other injuries: credential stuffing; phishing attacks; unsolicited emails, text messages, robocalls and other spam; mitigation costs; emotional distress; and diminution in value of the information taken.[13]

[13] Plaintiffs also allege "theft of their PII" and benefit of the bargain losses (SAC ¶¶ 142(a), 258) but do not address these alleged harms in their briefing. The Court declines to rule on issues not briefed by the parties. In any event, the Court is doubtful that either of these alleged injuries to be sufficiently concrete, as the SAC lacks any allegation that the information stolen was of any economic value *to plaintiffs*. Thus, it is unclear how plaintiffs suffered from "theft of their PII" apart from the other injuries discussed above, and without an exchange of value for the allegedly bargained-for data security, there can be no injury in fact based on a benefit of the bargain loss.

First, with respect to credential stuffing, phishing attacks, and the various forms of spam, the Court views these tactics as targeted *attempts* to commit identity theft. As stated above, the Court finds these attempts fall short of actual identity theft. Further, the source of these unsolicited contacts is hard to track. Even assuming that these acts are fairly traceable to the Zynga data breach, plaintiffs do not allege that any of these attempts succeeded, again something they would presumably know. Because these alleged harms merely present a risk of identity theft, they cannot plausibly be considered independent injuries.

Second, with respect to mitigation costs and emotional distress, Zynga argues that the risk of harm giving rise to these alleged injuries is "speculative," whereas plaintiffs contend that such risk is "substantial." (Mtn. at 10; Opp. at 12.) These injuries can only qualify as concrete injuries in fact when they are based on a risk of harm that is either "certainly impending" or "substantial." *See Clapper*, 568 U.S. at 422 (plaintiffs "cannot manufacture standing by incurring costs in anticipation of non-imminent harm"); *Payne v. Off. of the Cmm'r of Baseball*, 705 F. App'x 654, 655 (9th Cir. 2017) (rejecting argument that plaintiffs' "general anxiety about being injured by foul balls constitutes an injury-in-fact, because it is based on 'fears of hypothetical future harm that is not certainly impending'") (quoting *Clapper*, 568 U.S. at 416). Thus, no Article III standing exists if a plaintiff's theory of injury rests on an "attenuated chain of inferences necessary to find harm." *Clapper*, 568 U.S. at 414 n.5.

Given the nature of the information at issue, the Court agrees with Zynga and finds that the risk of harm which caused the asserted costs and stress is too conjectural such that they cannot qualify as concrete injuries of fact. For one thing, the Court questions whether criminals would be able to use e-mail addresses, Zynga usernames and Zynga passwords, Facebook username, phone numbers, and dates of birth, even collectively, to commit identity theft. The SAC does not allege that Zynga collected, or that plaintiffs stored in their accounts, their payment or other financial information. It is unclear how a third party could make a credit inquiry, set up a new bank account or access an existing one, apply for a loan, or commit some other fraud without more information, such as first and last names or social security number.

While the SAC alleges this information is susceptible to fraudulent use by way of phishing

attacks and credential stuffing, the Court finds this notion implausible. According to the SAC, the information stolen "includes enough information to potentially create targeted phishing attacks made up to look as they are an official communication from Zynga," (SAC ¶ 101) (internal quotation marks and citation omitted), but phishing, by its nature, demonstrates that the limited information disclosed is not enough. The Court would therefore still need to speculate that plaintiffs will be successfully duped by a phishing attack and that the additional information turned over as a result can be used to commit identity theft, which the SAC does not allege.

Credential stuffing also requires a series of assumptions to conclude that identity theft is substantially likely in this case. Johnson is the only named plaintiff whose plain text Zynga password was allegedly stolen and who used that same password "for many other online accounts, including her email account which she uses to send confidential information such as financial information and communications with her doctor's office." (SAC ¶ 20.) The SAC alleges that she and her sister "went through every online account she could think of that had the same password as her Zynga account." (*Id.*) I.C. also allegedly used his Zynga password "for approximately 90% of his online accounts, including email, entertainment, gaming, social media popular with youth, and others." (*Id.* ¶ 105.) Though the SAC does not allege that I.C.'s password was taken in plain text form, it does allege that online websites "explain[ed] how to crack the Zynga hashed passwords" (*id.* ¶ 72 (citations omitted)), which were already encrypted with an "outdated and insecure" encryption method. (*Id.* ¶ 71 (internal quotation marks and citation omitted).) I.C. also changed his account passwords and installed two-factor authentical application for his accounts but "cannot be certain" that he did this for all of his accounts. (*Id.* ¶ 118.)[14] The Court would therefore need to assume, at minimum, that (1) Johnson or I.C. have forgotten some account; (2) a third party could successfully access that account, for example, because plaintiffs paired the forgotten account's password with one of the other pieces of information taken in the breach; and (3) that other account could be used to consummate an unauthorized transaction. *See*, *e.g.*, *B.J.F.*

[14] Although Rosiak's Zynga hashed password was also allegedly taken, there is no allegation that he used the same password for his other accounts.

v. PNI Digital Media, No. 15-cv-1643 (MJP), 2016 WL 4014113, at *2 (W.D. Wash. July 27, 2016) (finding no standing even where the plaintiff alleged that she had used the same password because she did not "describe the nature of the accounts that she used the same password for" or "explain how she would be harmed if those other accounts were accessed by hackers"). The Court declines to find a "certainly impending" risk of harm based on a chain of unsupported inferences. Because plaintiffs do not show a substantial or imminent risk of identity theft, they cannot rely on the resulting mitigation expenses or emotional distress to secure standing.[15]

Third, with respect to the devaluation of the information stolen, the Court finds that plaintiffs do not adequately allege such an injury. "The Ninth Circuit has recognized diminution in value of personal theory as a viable theory of damages under state contract law." *Svenson v. Google Inc.*, No. 13-cv-4080 (BLF), 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016) (citing *Facebook Privacy Litig.*, 572 F. App'x 494, 494 (9th Cir. 2014). "In order to show injury in fact under this theory, [plaintiffs] must establish both the existence of a market for [their] personal information and an impairment of [their] ability to participate in that market." *Id.* (citing *In re Google, Inc. Privacy Policy Litig.*, No. 12-cv-1382 (PSG), 2015 WL 4317479, at *4 (N.D. Cal.

---

[15] Plaintiffs point to previous Ninth Circuit cases where the threat of identity theft constituted an injury in fact and argues that the Court should similarly find an injury in fact in this case. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1023 (9th Cir. 2018) (hackers' theft of "the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit-card and debit-card information of more than 2 million Zappos customers" constituted a substantial risk of future harm); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140, 1143 (9th Cir. 2010) (plaintiffs had alleged "a credible threat of harm" stemming from the theft of a laptop containing "the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees"). Indeed, this Court is aware that the Ninth Circuit in *Zappos* credited the plaintiffs' allegations that they were at a higher risk of "phishing" and "pharming" as a result of the data breach. *Zappos*, 888 F.3d at 1027. However, the information exposed in those cases provided the third parties with a clear ability to commit fraud or identity theft and therefore is distinguishable from the stolen information in the instant case, which, for the reasons stated above, the Court finds cannot, without more, plausibly be used to commit fraud.

More fundamentally, in light of *TransUnion*'s rejection of risk of harm as a basis for standing for damages claims, the Court questions the viability of *Krottner* and *Zappos*'s holdings finding standing on this very basis.

Finally, the Court is mindful of the procedural posture of *TransUnion*, as pointed out by plaintiffs, but does not consider the fact that *TransUnion* had proceeded to a jury verdict dictates a different result in this case. Indeed, at this stage, the Court accepts all the allegations as true and views them in the light most favorable to plaintiffs.

July 15, 2015)). Even assuming the existence of a market for the information taken in this case,[16] the SAC is devoid of any allegations describing how the breach devalued plaintiffs' specific information, that is, email addresses, Zynga usernames and passwords, phone numbers, dates of birth, or Facebook username, such that they are prevented from deriving economic benefit from this information in the future. *See*, *e.g.*, *In re Facebook, Inc. Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019) (plaintiffs failed to "plausibly allege that someone else would have bought [their non-disclosed personal information] as a stand-alone product"). "[P]laintiffs' economic-loss theory is therefore purely hypothetical and does not give rise to standing." *Id.* (citing cases).

In sum, plaintiffs have not alleged that they were victims of actual identity theft, nor have they pled any other injuries caused by the risk of identity theft that are sufficiently concrete. Accordingly, under *TransUnion*, plaintiffs fail to allege standing to sue for damages and therefore all such claims are **DISMISSED**.

b. STANDING TO SUE FOR INJUNCTIVE RELIEF

The Court also must consider whether plaintiffs have standing to request injunctive relief. As stated above, a "person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *TransUnion*, 141 S. Ct. at 2210 (citing *Clapper*, 568 U.S. at 414 n.5); *see also Bates v. United Parcel Service, Inc.*, 511 F.3d 974, 985 (standing inquiry for injunctive relief requires plaintiffs to "demonstrate that [they have] suffered or [are] threatened with a 'concrete and particularized' legal harm, coupled with a 'sufficient likelihood that [they] will again be wronged in a similar way.") (quoting *Lujan*, 504 U.S. at 560, and *City of Los Angeles*, 461 U.S. 95, 111 (1983)). Zynga argues that plaintiffs "cannot show any imminent risk of future

[16] Plaintiffs' counsel offers a declaration attesting to both the underground and legitimate "marketplaces through users can monetize their personal information." (Declaration of Mark Clifford in Support of Opposition to Motion to Dismiss, Dkt. No. 98-1, ¶ 22.) The declaration attaches an expert report filed in another case which "highlight[s] the various means by which the value of compromised PII may be calculated and how consumers themselves can realize this value" and notes that "[t]he types of PII described in [the] report are some of the same types of PII compromised in the Zynga data breach." (*Id.* ¶¶ 23–27.) None of these averments, however, are included in the SAC, nor do they address plaintiffs' specific information.

harm from *this* data breach." (Mot. at 19.) For the reasons stated in Section III.B.2.a.ii, the Court agrees. Because the risk of harm here is not sufficiently imminent or substantial to confer standing, not even for a claim seeking purely injunctive relief, the Court **DISMISSES** all such claims.[17]

IV. CONCLUSION

In short, plaintiffs fail to allege a concrete injury in fact and therefore lack constitutional standing to pursue their claims in federal court. The Court does not take lightly the serious harm suffered when one's identity is stolen, especially that of a minor, and does not suggest that a plaintiff must always wait until this happens before seeking relief in federal court following a data breach. However, not every data breach creates a concrete injury, particularly where, as here, the information allegedly stolen has not be shown to be either so private that a reasonable person would be offended if exposed or so sensitive that it could be enough to commit identity theft.

Plaintiffs have already amended their pleadings after Zynga's prior motion to dismiss, and they fail to show how amendment could demonstrate a cognizable injury suffice to support Article III standing. Because Article III standing is an essential ingredient for subject matter jurisdiction in federal court, the motion to dismiss for lack of subject matter jurisdiction is **GRANTED**, and the case is **DISMISSED WITH PREJUDICE**.[18]

This Order terminates Docket Number 96 and closes the case.

IT IS SO ORDERED.

Dated: April 29, 2022

YVONNE GONZALEZ ROGERS
UNITED STATES DISTRICT COURT JUDGE

[17] Plaintiffs correctly point out that Zynga does not challenge their standing for declaratory relief. Notwithstanding, the Court has an independent obligation to confirm its subject matter jurisdiction. *See FW/PBS*, 493 U.S. at 231. For the same reason that plaintiffs lack standing to pursue injunctive relief, namely, failure to demonstrate that the asserted risk of harm is sufficiently imminent or substantial, the Court concludes that they also lack standing to pursue declaratory relief.

[18] In reaching its decision, the Court did not have to rely on any matters contained in Zynga's request for judicial notice or plaintiffs' administrative motion to file a surreply. (Dkt. Nos. 97, 103.) Accordingly, those requests are **DENIED AS MOOT.**